



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,302	02/28/2002	Alexander Medvinsky	018926-008400US	2065

7590 09/28/2006

Motorola, Inc.  
Robert P. Marley  
Broadband Communications Sector  
101 Tournament Drive  
Horsham, PA 19044

EXAMINER

GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/086,302		MEDVINSKY, ALEXANDER	
	<b>Examiner</b>		<b>Art Unit</b>	
	Shewaye Gelagay		2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 31 August 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-6, 8-12, 18-22 and 24-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-12, 18-22 and 24-26 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 31, 2006 has been entered.

2. Claims 1-6, 8-12, 18-22 and 24-26 are pending.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-6, 8, 11-12, 18-22 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yang United States Letter Patent Number 6,069,877 in view of Brezak et al. (hereinafter Brezak) U.S. Publication Number 2002/0150253.

As per claim 1:

Yang discloses a method for detecting clones (unauthorized duplicate identities) of the client, the method comprising:

forwarding a first signal from a client, the first signal for requesting access to a server; (Col. 2, lines 44-61; Col. 3, lines 39-45 and lines 59-60; Col. 10, lines 43-45)

verifying that the client is authorized to access the server; (Col. 4, lines 4-5)

receiving a second signal from an entity, the second signal for requesting access to the server, wherein the entity has identifying information identical to the client; (Col. 4, lines 6-9) and

if the second request is received prior to expiration of the time T, either marking the entity as a possible clone or denying the second request in order to prevent access to the server. (Col. 2, line 45; Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang discloses if the identification code of the second unit is an apparent duplicate of the first unit and if the first unit has already registered, refusing the registration of the second unit. (Col. 4, lines 9-14) Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T.

Brezak in analogous art, however, disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T. (page 4, paragraph 56, page 5, paragraphs 59-60 and 65)

Art Unit: 2137

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

As per claim 2:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a method wherein the encrypted session key is valid for a designated duration. (Page 4, paragraph 55)

As per claim 3:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a method wherein the designated duration is for determining the time T for which the authentication token is valid. (Page 4, paragraph 55)

As per claims 4 and 18:

Yang teaches a system for detecting clones of a client within a communication network, the system comprising:

an application server communicably; (Figure 1, Col. 3, line 39)

a client for providing a first request to access the application server; (Figure 1, Col. 3, lines 37-38)

receiving a second request to access the application server, the second request being received from an entity having identifying information identical to the client; (Col. 4, lines 6-9) and

if the second request is received during time T, denying the second request to prevent the entity from accessing the application server. (Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

In addition, Yang discloses if the identification code of the second unit is an apparent duplicate of the first unit and if the first unit has already registered, refusing the registration of the second unit. (Col. 4, lines 9-14) Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T.

Brezak in analogous art, however, disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token

is valid for a time T. (page 4, paragraph 56, page 5, paragraphs 59-60 and 65)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

As per claim 5:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Yang further discloses a system wherein the entity is a clone. (Col. 2, line 45)

As per claims 6, 24 and 25:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Yang further discloses a system wherein the identifying information is a client identifier copied by the clone. (Col. 3, lines 1-4)

As per claim 8:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system comprising the client deriving a copy of the session key for accessing the application server. (Page 4, paragraphs 56-57)

As per claims 11, 12 and 20:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system comprising using a

Art Unit: 2137

key algorithm for authenticating communication between the KDC and the client such that all clients wishing access to the server are required to contact the KDC. (Page 4, paragraphs 56-57)

As per claim 21:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system wherein a ticket granting server is the server, and the ticket is a ticket granting ticket. (Page 4, paragraphs 56-58)

As per claim 22:

Yang teaches a method for detecting clones in a communication network, the method comprising:

receiving a request to access the KDC, the request being received from an entity with the same identifying information as the authorized client; (Col. 4, lines 6-9) and

if the request is received during time T, flagging the entity as a possible clone or denying the request to access. (Col. 2, line 45; Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and providing a an authentication token including an encrypted session key to an authorized client, the authentication token for accessing a KDC, the session key valid for a time duration T.



Brezak in analogous art, however, discloses a KDC and providing a an authentication token including an encrypted session key to an authorized client, the authentication token for accessing a KDC, the session key valid for a time duration T. (page 4, paragraph 56, page 5, paragraphs 59-60 and 65) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

As per claim 26:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system wherein the KDC is the server. (Page 3, paragraph 42)

5. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yang United States Letter Patent Number 6,069,877 in view of Brezak et al. (hereinafter Brezak) U.S. Publication Number 2002/0150253 further in view of Tung et al. Public Key Cryptography for Initial Authentication in Kerberos, Internet Draft, (hereinafter Tung).

As per claim 9:

The combination of Yang and Brezak discloses all the subject matter as discussed above. Both references do not explicitly disclose a system wherein the encrypted session key is derived using a key agreement algorithm.

Tung in analogous art, however, discloses a system wherein the session key is derived using a key agreement algorithm. (Section 2, paragraph 2)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang and Brezak to include a system wherein the session key is derived using a key agreement algorithm. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Tung (Section 2, paragraph 4) in order to enable access to Kerberos-secured services based on initial authentication using public key cryptography.

As per claim 10:

The combination of Yang, Brezak and Tung disclose all the subject matter as discussed above. In addition, Tung further discloses a system wherein the key agreement algorithm is the Diffie-Hellman algorithm. (Section 2, paragraph 3)

### ***Response to Arguments***

6. Applicant's arguments filed on 8/31/06 have been considered but are moot in view of the new ground(s) of rejection.

The applicant argued the examiner did not explicitly reject claim 4. The examiner would like to point out there were two amendments filed (one signed by attorney Lawrence T. Cullen submitted first and another signed by attorney Stephen F. Jewett submitted second) the examiner considered the later in which claim 4 is presented as cancelled and new claim 27 is added.

**Conclusion**

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER